UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,079	02/19/2004	Stephen James Crane	B-5374 621705-3	4686

7590 09/13/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
09/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,079	CRANE ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/19/2004, 05/24/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response of the original filing of February 19, 2004. Claims 1-24 are pending and have been considered below.

Drawings

2. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

3. Claim 1 is objected to because of the following informalities: line 8 recites the limitation of "the later" the examiner suggests the use of "said party" instead.

4. Claim 35 is objected to because of the following informalities: line 4 recites the limitation of "the later" the examiner suggests the use of "said second party" instead.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> a. The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1 recites the limitation "the authority" in line 9. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. The claimed invention is directed to non-statutory subject matter. The claims recite the limitation of "computing entity associated ... and arranged " without taking any further action. Thus, claims 24-38 are drawn to a computer program per se. A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine or manufacture. A computer program is not a combination of substances and therefore not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-38 are rejected under 35 U.S.C. 102(e) as being anticipated by **Kacker et al** (US 7003117).

Claims 1, 24: **Kacker et al** discloses a method and a system for limiting a service to members of a group who are registered with a membership authority (policy enforcement service) (Fig. 1), the method and the system comprising:

i. A first computer entity (the combination of data packaging service 16, content providers 14, and distribution services 18) (column 10, lines 57-65 and Fig 1) associated with a provider of said service and arranged to encrypt data based on encryption parameters comprising public data provided by the membership authority (first input made up of public parameters received from policy enforcement service)(column 7, lines 5-45) and an encryption key string (receiver's identity), and to provide the encrypted data to a party(the encrypted data is securely communicated to users at user device)(column 2, lines 10-35; column 7, lines 45-67; Fig. 3 and Fig.5);

ii. A second computer entity associated with said party and arranged to decrypt the encrypted data using a decryption key obtained from the membership authority (once the user has obtained the private key, the user uses an identity-based description engine to decrypt the encrypted data) (column 3. lines 50-63; column 8, lines 25-65; Fig. 4); and

a third computing entity associated with the membership authority and comprising:

(1) A membership-checking arrangement for checking whether said party is registered

with the authority as a member of said group (the access request includes information on the characteristics of the user (e.g. user age, membership status, security clearance etc..) (Column 37-51; Fig. 2),

iii. A key-generation arrangement for generating the decryption key in dependence on

said encryption key string and private data related to said public data (the access request directs the policy enforcement service to provide the private key corresponding to the public key that was used to encrypt data) (column 8, lines 53-64; Fig. 2), and

iv. A control arrangement for enabling the generation of the decryption key by the key-generation arrangement and/or the provision of the decryption key to the second computer entity, only if said party is a group member as checked by the membership-checking arrangement (column 8 line 65 to column 9 line 17).

Claims 2, 25: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the encryption key string is created in whole or in part by the service provider (the policy enforcement service 20 may create a master secret from a number that is randomly generated at the service by a processor housed inside a tamper-proof

enclosure. The master secret is subsequently used by the policy enforcement service 20 to generate private keys for users 22 in the system to use in decrypting encrypted data and to generate public parameter information for use by data packaging service 16 in encrypting data prior to distribution)(column 11 line 10 to column 12 line 24; Fig. 2).

Claims 2, 26: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the encryption key string is created in whole or in part by the service provider upon receipt of a service request from said party (column 11 line 10 to column 12 line 24; Fig. 2), the requesting party receiving the encryption key string from the service provider and providing it to the membership authority, and the membership authority only returning the decryption key after confirming that the party is a registered group member (the user uses policy information that has been received from the data packaging service as the basis for the access request. The access request (or a follow-up communication between the user and the policy enforcement service) includes information on the characteristics of the user (e.g., user age, membership status, security clearance, etc)(column 8 line 37 to column 9 line 16;column 12 line 44 to column 13 line 26; Fig. 2).

Claims 4, 27: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the party creates the encryption key string and provides it to the service provider when requesting said service, the party obtaining the decryption key from the

membership authority either before or after requesting said service from the service provider (column 12 line 44 to column 13 line 26);

Claims 5, 28: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 4 and 27 above, and further discloses that the encryption key string is formed using information about at least one of said party and the membership authority, this information being used by the service provider in the process of determining whether to provide said service to said party (column 13, lines 27-43).

Claims 6, 29: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the encryption and decryption keys are created by the membership authority and provided to said party on the latter becoming a registered member of said group (the policy enforcement service 20 may create a master secret from a number that is randomly generated at the service by a processor housed inside a tamper-proof enclosure. The master secret is subsequently used by the policy enforcement service 20 to generate private keys for users 22 in the system to use in decrypting encrypted data and to generate public parameter information for use by data packaging service 16 in encrypting data prior to distribution)(column 11 line 10 to column 12 line 24; Fig. 2).

Claims 7, 30: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 6 and 29 above, and further discloses that the encryption key string is formed using information about at least one of said party

and the membership authority, this information being used by the service provider in the process of determining whether to provide said service to said party (column 13, lines 27-43).

Claims 8, 10, 13, 31, 33: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the data that is encrypted by the service provider is a data component of the service, said party only being able to decrypt and use this data component if it is a registered member of said group (column 8 line 65 to column 9 line 17).

Claims 9, 32: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 8 and 31 above, and further discloses that the data component comprises at least one of software and digital media content (The content that is distributed using system 10 may be media (e.g., digital video or audio), business record data (e.g., stock sales data, banking or other financial records, supply chain data, etc.), software (e.g., games or other applications), or any other suitable data) (column 5, lines 40-59).

Claims 11, 34: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that in order to obtain the decryption key from the membership authority, said party proves its identity to the membership authority by using a secure entity authentication protocol During user authentication, the policy enforcement

service may use this multiple-attribute policy information and information on the characteristics of a given user who is requesting access to the encrypted data (e.g., age=30 and studio membership status=Sony) to determine whether or not to provide the requesting user with the private key needed to decrypt the encrypted data) (column 8, lines 6-27; Fig. 4 seep 50 and step 52).

Claims 12, 35: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 11 and 34 above, and further discloses that the entity authentication protocol uses a secret that is securely stored in a trusted computing platform the integrity of which is checked by the membership authority before it accepts the proof of identity provided by said party (At step 24 of FIG. 2, policy enforcement service 20 of FIG. 1 obtains a master secret s. For example, the policy enforcement service 20 may create a master secret from a number that is randomly generated at the service by a processor housed inside a tamper-proof enclosure)(column 11, lines 10-28; Fig. 2).

Claims 14, 36: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the cryptographic processes involving said encryption and decryption keys are identifier-based cryptographic processes utilizing quadratic residuosity (column 7, lines 10-15).

Claims 15, 37: **Kacker et al** discloses a method and a system for limiting a service to members of a as in claims 1 and 24 above, and further discloses that the cryptographic processes involving the said encryption and decryption keys

are identifier-based cryptographic processes utilizing Weil or Tate pairings (column 7, lines 10-20).

Claim 16: **Kacker et al** discloses a method for limiting a service to members of a as in claim 1 above, and further discloses that multiple groups are registered with the membership authority with each group having respective associated said public and private data (column 8, lines 53-64; Fig. 2), the service provider encrypting the data to be provided to said party using the public data of the group to which the service provider requires that party to belong in order to receive the service (column 8, lines 53-64; Fig. 2), this group being identified to the membership authority to enable it to check the party's membership of that group and to provide the appropriate decryption key by using the private data associated with that group when generating the decryption key (column 8, lines 27-65).

Claim 17: **Kacker et al** discloses a method for limiting a service to members of a as in claim 1 above, and further discloses that multiple groups are registered with the membership authority and the same said public and private data is used in respect of all groups (column 8, lines 53-64; Fig. 2), the service provider encrypting the data to be provided to the requesting party using an encryption key string formed using at least an identifier of the group to which the service provider requires that party to belong in order to receive the service (column 8, lines 53-64; Fig. 2), the membership authority determining from the encryption key string the group in respect of which it is to check the membership of said

party before it provides the decryption key to

that party(column 8, lines 27-65).

Claim 18: **Kacker et al** discloses a method for limiting a service to members of a as in claim 1 above, and further discloses that the service provider provides the service to members of said group as a result of a prior arrangement with the group representatives (column 8, lines 52-65).

Claim 19: **Kacker et al** discloses a method for limiting a service to members of a as in claim 1 above, and further discloses that the service provider provides the service to parties meeting a particular condition, the service provider providing the service to members of said group after having determined that said condition is a predetermined membership requirement of said group (Column 8 line 65 to column 9 line 17).

Claim 20: **Kacker et al** discloses a method for limiting a service to members of a as in claim 1 above, and further discloses that a service provider to limit service access to parties meeting multiple conditions each of which corresponds to a predetermined membership requirement of a different group whose members are registered with an associated membership authority, as applied in to check each condition using the said public and private data appropriate for the group that has the corresponding membership requirement (column 13 line 27to column 14 line 25).

Claim 21: **Kacker et al** discloses a method for limiting a service to members of a as in claim 20 above, and further discloses that for each group of which the party

is required to be a member to access the service, the service provider encrypts a different item of data to be provided to said party (column 3, lines 34-62).

Claim 22: **Kacker et al** discloses a method for limiting a service to members of a as in claim 20 above, and further discloses that the data encrypted in respect of one condition is used as the data to be encrypted in respect of the next condition, the encrypted data resulting from the encryption effected in respect of all said conditions then being provided to the requesting party for decryption in successive decryption operations (column 3, lines 10-63)

Claim 23: **Kacker et al** discloses a method for limiting a service to members of a as in claim 20 above, and further discloses that the service provider encrypts the data to be provided to said party using public data associated with each of the relevant groups,

decryption of the encrypted item only being possible by obtaining a decryption sub-key in respect of each group from the corresponding membership authority (column 8, lines 27-65).

Claim 38: **Kacker et al** discloses a computing entity comprising:

v. A first data store for holding private data (column 10, lines 57-65 and Fig 1);

vi. A second data store for holding membership data indicative of members of a group (column 3. lines 50-63; column 8, lines 25-65; Fig. 4);

vii. A membership-checking arrangement for checking whether a particular party is a member of said group arrangement (column 8 line 65 to column 9 line 17),

viii. A communications interface for receiving an encryption key string from a party requesting the corresponding decryption key, and for outputting the requested decryption key to the requesting party (column 12, lines 55-64);

ix. A decryption-key generation unit for using the private data and a received encryption key string to generate a corresponding decryption key for decrypting data encrypted using the encryption key string and public data derived using said private data (column 12 line 44 to column 13 line 26);

x. A control arrangement for enabling the generation of the decryption key by the decryption-key generation arrangement and/or the provision of the decryption key to a said requesting party via said communications interface, only if that party is a group member as checked by the membership-checking arrangement (column 8 line 65 to column 9 line 17).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. **Andivahis et al** US 7146009 Secure electronic messaging system requiring key retrieval for deriving decryption keys.

b. **Boneh et al** US 7113594 System and methods for identity based encryption techniques related cryptographic techniques.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday September 07, 2007

Nassar G. Moazzami
Supervisory Patent Examiner

9,7,07